Research Field And Department	Computer Security / Computer Science Department
Supervisor	Pedro Peris-López / Carmen Cámara ({pperis,macamara}@inf.uc3m.es)
Title of the Work	Design, Formal Analysis, and Hardware Implementation of Lightweight and AI-Enhanced Cryptographic Protocols

Abstract:
This research focuses on the design, analysis, and implementation of lightweight cryptographic protocols and primitives aimed at securing Internet of Things (IoT), vehicular, and industrial networks. The work emphasizes efficiency, privacy, and robustness, addressing the unique constraints of embedded and resource-limited devices.

The project covers the complete cryptographic development lifecycle — from protocol design to informal and formal security analysis, computational and energy evaluation, and hardware implementation — while also exploring pseudo-random number generators (PRNGs) as fundamental cryptographic components.

The expected outcome is a set of secure, verified, and hardware-efficient cryptographic mechanisms applicable to modern embedded ecosystems that integrate AI-driven and adaptive security paradigms.

Main Tasks to Carry Out:

1. Design of Cryptographic Protocols
   - Development of secure and lightweight authentication and key-establishment schemes for IoT, vehicular, and industrial communication systems, to mention some application scenarios.
   - Exploration of AI-based optimization and anomaly detection techniques to improve adaptability and resilience of cryptographic mechanisms in dynamic environments.
2. Informal Analysis of Cryptographic Protocols
   - Identification of vulnerabilities such as replay, impersonation, and desynchronization attacks.
   - Comparative analysis of contemporary lightweight and AI-enhanced protocols targeting computationally constrained devices.
3. Formal Analysis of Cryptographic Protocols
   - Formal verification of properties such as secrecy, authenticity, and freshness using ProVerif, Scyther, and Tamarin.
   - Validation under standard adversarial and oracle-based models (e.g., Real-or-Random).
4. Computational, Memory, and Energy Evaluation
   - Quantitative assessment of computational cost, memory footprint, and power efficiency.
   - Comparison with the state of the art in lightweight and AI-enhanced cryptographic schemes.

5. Hardware Implementation

- FPGA or SoC implementation of the proposed protocols optimized for low area, latency, and energy.
- Validation on embedded testbeds relevant to IoT and vehicular communication systems.

6. Design of Cryptographic Primitives: PRNGs

- Development of secure, efficient pseudo-random number generators (PRNGs) suitable for resource-constrained hardware.
- Exploration of entropy sources, including behavioral and physiological data, to strengthen randomness generation.

7. Randomness and Entropy Analysis

- Validation of PRNGs using standard statistical test suites such as NIST SP 800-22 and Dieharder.
- Entropy estimation and randomness quality assessment to ensure compliance with cryptographic standards.

References/Bibliography if required

1. Geranfar, H., Abolhassani, B., Bagheri, N., Javadi, A., Peris-López, P., Cámara, C., & Kumari, S. (2025). An enhanced security protocol for vehicular ad hoc networks. IEEE Internet of Things Journal, 12(17), 35207–35225. https://doi.org/10.1109/JIOT.2025.3579986
2. Ramos, A., Cámara, C., Martín, H., & Peris-López, P. (2025). AI-driven device fingerprinting using on-chip monitoring sensors: A novel time-series-based approach. IEEE Sensors Journal, 25(7), 12064–12075. https://doi.org/10.1109/JSEN.2025.3539571
3. Bagheri, N., Kumari, S., Cámara, C., & Peris-López, P. (2022). Defending Industry 4.0: An enhanced authentication scheme for IoT devices. IEEE Systems Journal, 16(3), 4501–4512. https://doi.org/10.1109/JSYST.2021.3131689
4. Safkhani, M., Cámara, C., Peris-López, P., & Bagheri, N. (2021). RSEAP2: An enhanced version of RSEAP, an RFID-based authentication protocol for vehicular cloud computing. Vehicular Communications, 28, 100311. https://doi.org/10.1016/j.vehcom.2020.100311
5. Cámara, C., Martín, H., Peris-López, P., & Entrena, L. (2020). A true random number generator based on gait data for the Internet of You. IEEE Access, 8, 71642–71651. https://doi.org/10.1109/ACCESS.2020.2986822
6. Peris-López, P., & Cámara, C. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 55, 272–289. https://doi.org/10.1016/j.jbi.2015.04.007